

WHAT IS CLAIMED IS:

1           1.     A hardware authenticity verification system, comprising:  
2                     a hardware element having a hardware address;  
3                     a digital signature generator to create a digital signature of the hardware  
4                     address of the hardware element;  
5                     a memory element to store the digital signature of the hardware element;  
6                     and  
7                     a software program to compare the digital signature of the hardware  
8                     element to a known value.

1           2.     The hardware authenticity verification system according to claim 1,  
2                     wherein the software program is a device driver.

1           3.     The hardware authenticity verification system according to claim 1,  
2                     wherein a device driver decrypts the digital signature of the hardware element  
3                     that is stored in the memory element.

1           4.     The hardware authenticity verification system according to claim 1,  
2                     wherein the hardware element is a network adapter.

1           5.     The hardware authenticity verification system according to claim 1,  
2                     wherein the digital signature generator manipulates the hardware address of the  
3                     hardware element with a hash algorithm.

1 6. The hardware authenticity verification system according to claim 1,  
2 wherein the digital signature generator encrypts the hardware address of the  
3 hardware element with a private key.

1 7. The hardware authenticity verification system according to claim 1,  
2 wherein the hardware authenticity verification system is included in a data  
3 processing device.

1 8. A network device, comprising:  
2 a microprocessor;  
3 a user interface to receive information from a user;  
4 a power supply to supply power to the network device; and  
5 a hardware authenticity verification system, including  
6 a hardware element having a hardware address,  
7 a digital signature generator to create a digital signature of the  
8 hardware address of the hardware element,  
9 a memory element to store the digital signature of the hardware  
10 element, and  
11 a software program to compare the digital signature of the  
12 hardware element to a known value.

1 9. The network device according to claim 8, wherein the software program is  
2 a device driver.

1 10. The network device according to claim 8, wherein a device driver decrypts  
2 the digital signature of the hardware element that is stored in the memory  
3 element.

1 11. The network device according to claim 8, wherein the hardware element is  
2 a network adapter.

1 12. The network device according to claim 8, wherein the digital signature  
2 generator manipulates the hardware address of the hardware element with a  
hash algorithm.

1 13. The network device according to claim 8, wherein the digital signature  
2 generator encrypts the hardware address of the hardware element with a private  
key.

1 14. A network system, comprising:  
2 a first data processing device;  
3 a second data processing device;  
4 a communication device to enable the first data processing devices to  
5 communicate with the second data processing device; and  
6 a hardware authenticity verification system, including  
7 a hardware element having a hardware address,

8 a digital signature generator to create a digital signature of the  
9 hardware address of the hardware element,  
10 a memory element to store the digital signature of the hardware  
11 element, and  
12 a software program to compare the digital signature of the  
13 hardware element to a known value.

1 15. The network system according to claim 14, wherein the software program  
2 is a device driver.

3 16. The network system according to claim 14, wherein a device driver  
4 decrypts the digital signature of the hardware element that is stored in the  
5 memory element.

6 17. The network system according to claim 14, wherein the hardware element  
7 is a network adapter.

8 18. The network system according to claim 14, wherein the digital signature  
9 generator manipulates the hardware address of the hardware element with a  
10 hash algorithm.

1 19. The network system according to claim 14, wherein the digital signature  
2 generator encrypts the hardware address of the hardware element with a private  
3 key.

1 20. The network system according to claim 14, wherein the hardware  
2 authenticity verification system is included in the first data processing device.

1 21. The network system according to claim 14, wherein at least one of the first  
2 data processing device and the second data processing device is a computer.

1 22. A method of verifying authenticity of a hardware element, comprising:  
2 creating a digital signature of a hardware address of the hardware  
3 element;  
4 storing the digital signature of the hardware address of the hardware  
5 element in a memory element;  
6 comparing the digital signature of the hardware element to a known value;  
7 and  
8 permitting access to the hardware element only if the digital signature of  
9 the hardware element is same as the known value.

1 23. The method according to claim 22, wherein the method further includes  
2 decrypting the digital signature of the hardware element that is stored in the  
3 memory element.

1 24. The method according to claim 22, wherein the method further includes  
2 storing the hardware address of the hardware element in the memory element.

1 25. The method according to claim 22, wherein the method further includes  
2 manipulating the hardware address of the hardware element that is stored in  
3 memory with a hash algorithm.

1 26. The method according to claim 22, wherein the hardware element is a  
2 network adapter.

1 27. The method according to claim 22, wherein creating the digital signature  
2 includes manipulating the hardware address of the hardware element with a hash  
3 algorithm.

1 28. The method according to claim 22, wherein creating the digital signature  
2 includes encrypting the hardware address of the hardware element with a private  
3 key.

1 29. A hardware authenticity verification system, comprising:  
2 a machine-readable storage medium; and  
3 machine-readable program code, stored on the machine-readable storage  
4 medium, the machine-readable program code having instructions to

5                   create a digital signature of a hardware address of the hardware  
6                   element;  
7                   store the digital signature of the hardware address of the hardware  
8                   element in a memory element;  
9                   compare the digital signature of the hardware element to a known  
10                  value; and  
11                  permit access to the hardware element only if the digital signature  
12                  of the hardware element is the same as the known value.

30.    The hardware authenticity verification system according to claim 29,  
wherein the machine-readable program code further includes instructions to  
decrypt the digital signature of the hardware element that is stored in the memory  
element.

31.    The hardware authenticity verification system according to claim 29,  
wherein the machine-readable program code further includes instructions to store  
the hardware address of the hardware element in the memory element.

32.    The hardware authenticity verification system according to claim 29,  
wherein the machine-readable program code further includes instructions to  
manipulate the hardware address of the hardware element that is stored in  
memory with a hash algorithm.

1        33.    The hardware authenticity verification system according to claim 29,  
2        wherein the hardware element is a network adapter.

1        34.    The hardware authenticity verification system according to claim 29,  
2        wherein the machine-readable program code further includes instructions to  
3        manipulate the hardware address of the hardware element with a hash algorithm.

1        35.    The hardware authenticity verification system according to claim 29,  
2        wherein the machine-readable program code further includes instructions to  
3        encrypt the hardware address of the hardware element with a private key.